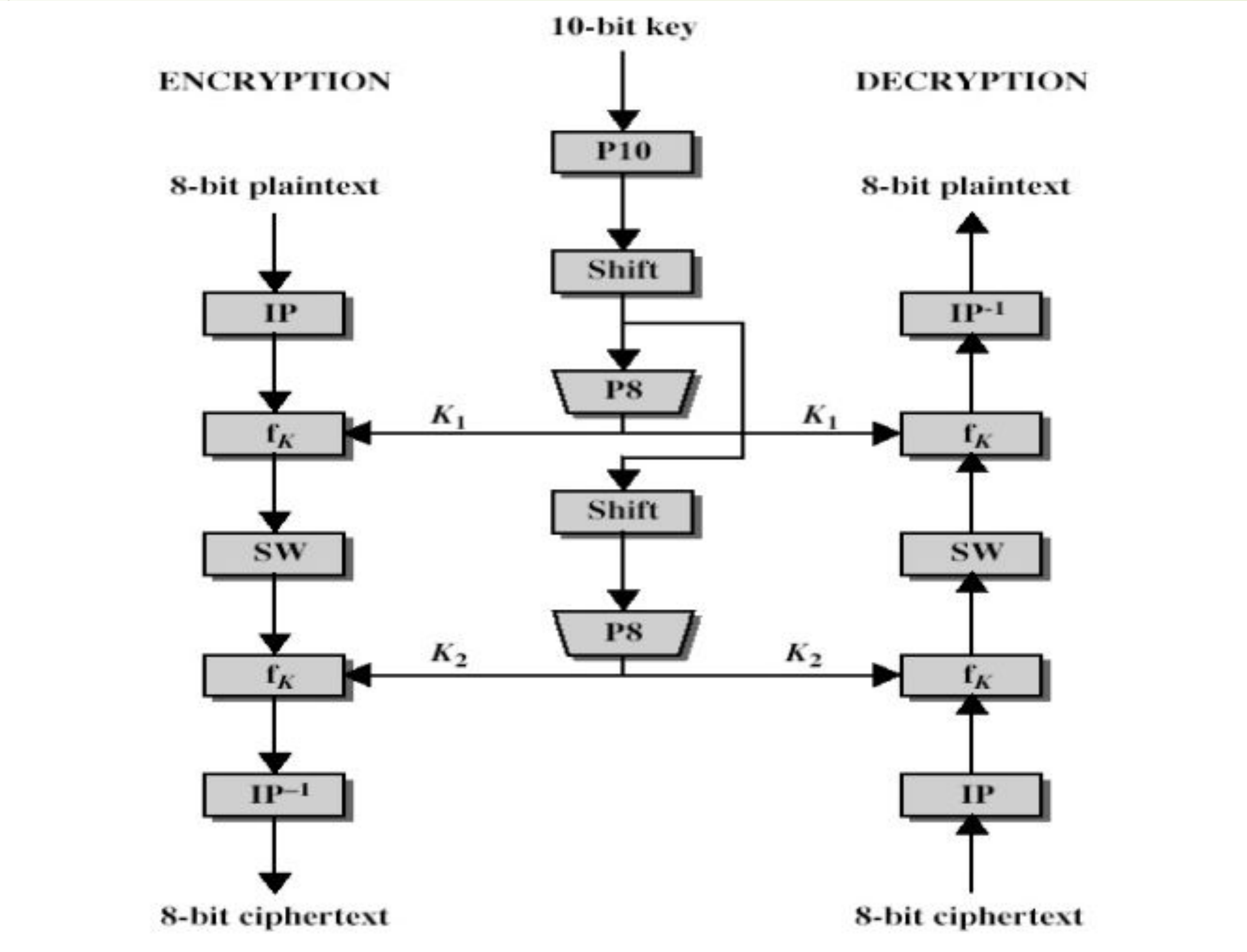
Data Encryption Standard (DES)

Outline

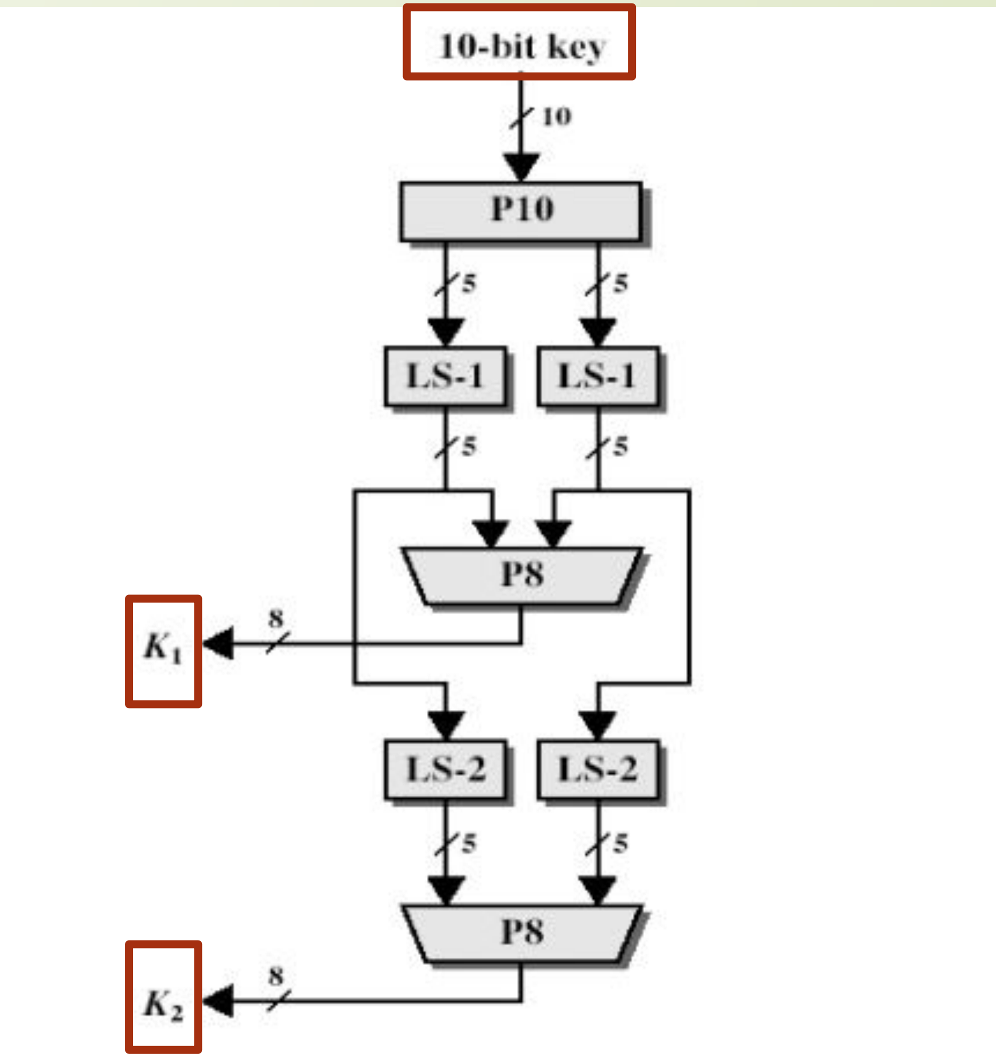
- S-DES
- DES

Simplified DES



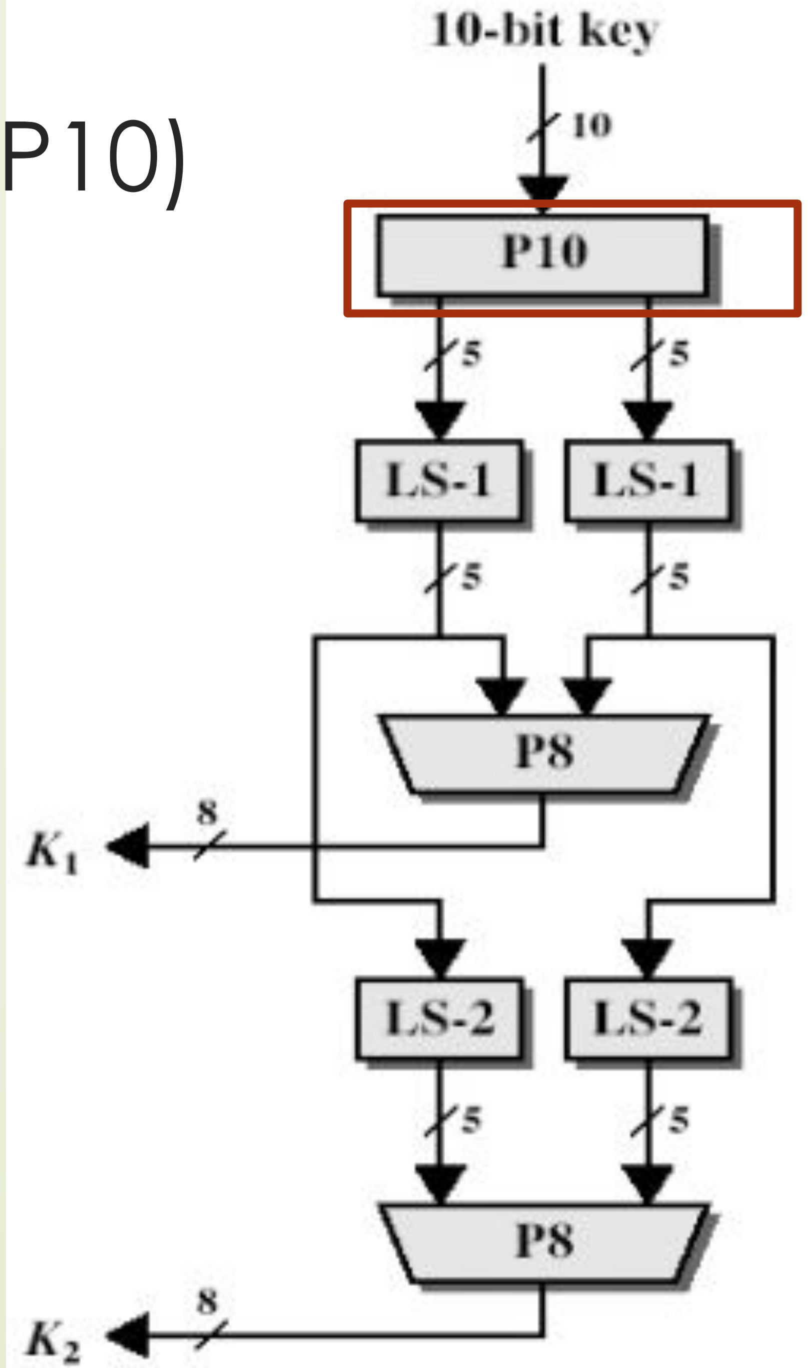
S-DES Key Generation

- S-DES depends on the use of a 10-bit key shared between sender and receiver.
- From this key, two 8-bit sub keys are produced for use in particular stages of the encryption and decryption algorithm.



Step 1 : Initial Permutation (P10)

P10									
3	5	2	7	4	10	1	9	8	6



Step 1 : Initial Permutation (P10)

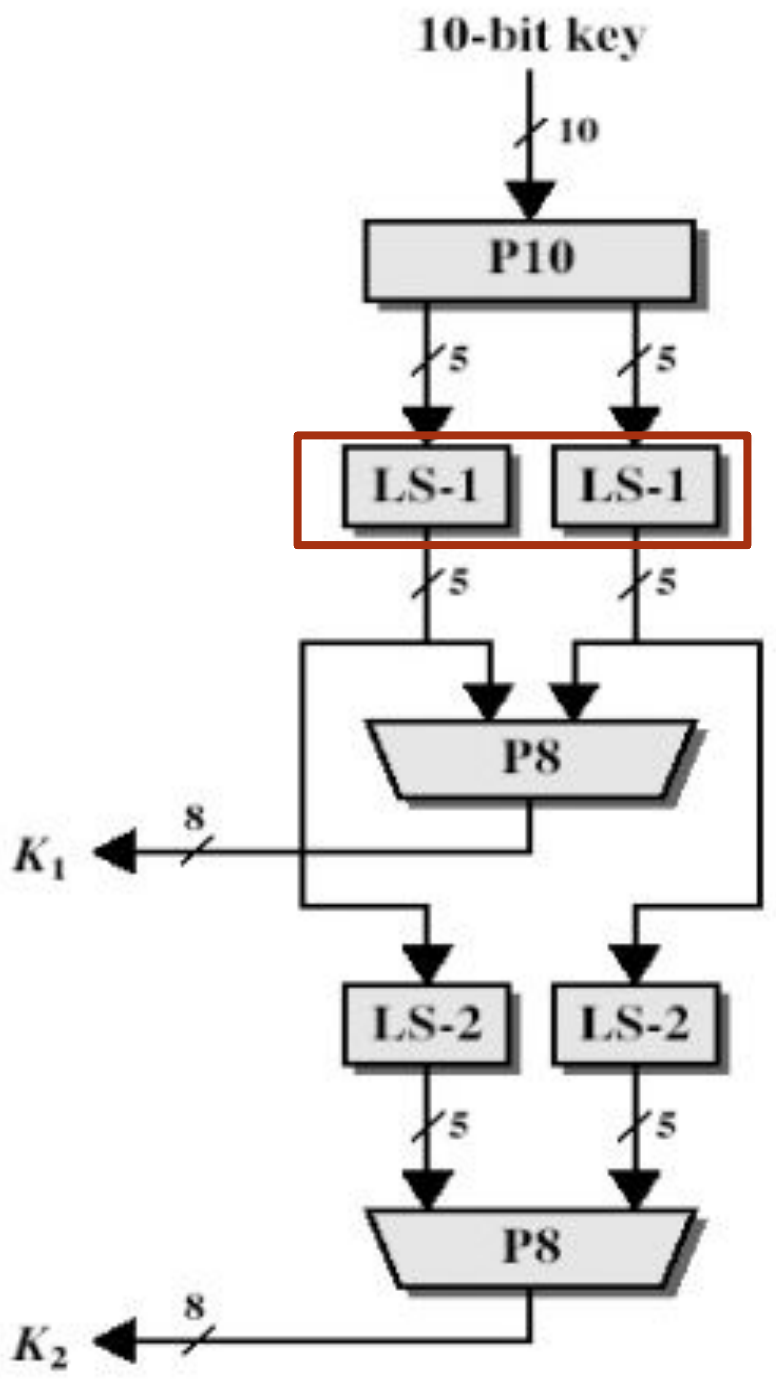
P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) =
(k3, k5, k2, k7, k4, k10, k1, k9, k8, k6)

P10									
3	5	2	7	4	10	1	9	8	6

- This table is **read from left to right.**
- Each position in the table gives the identity of the input bit that produces the output bit in that position.
- The **first output** bit is **bit 3 of the input**;
- The **second output** bit is **bit 5 of the input**, and so on.

Step 2 a circular left shift (LS-1) or rotation

- For example, **the key (1010000010)** is permuted to **(1000001100) after First Step**.
- Next, **perform a circular left shift (LS-1)**, or rotation, separately on the first five bits and the second five bits.
- **The result is (00001 11000).**

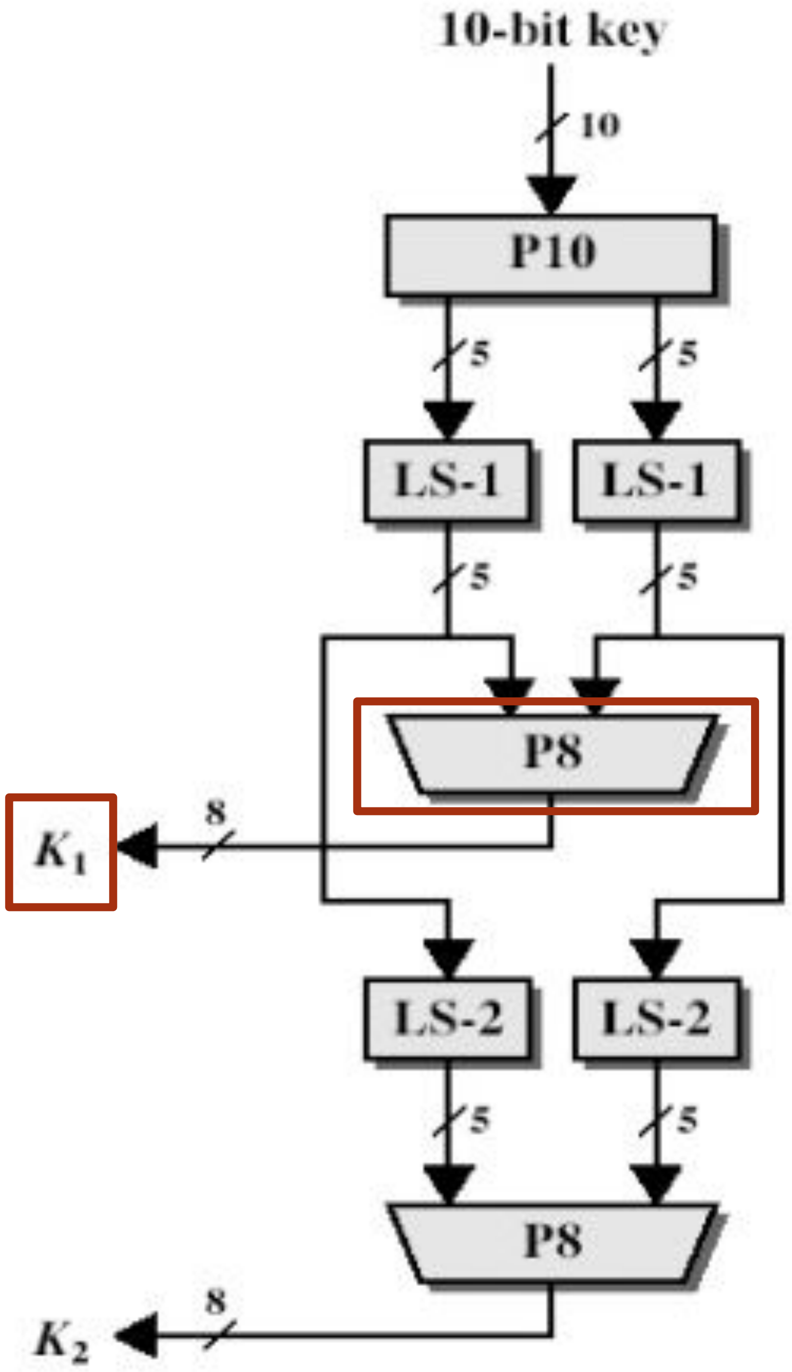


Step 3: Permutation (P8)

- P8 picks out and permutes 8 of the 10 bits according to the following rule.

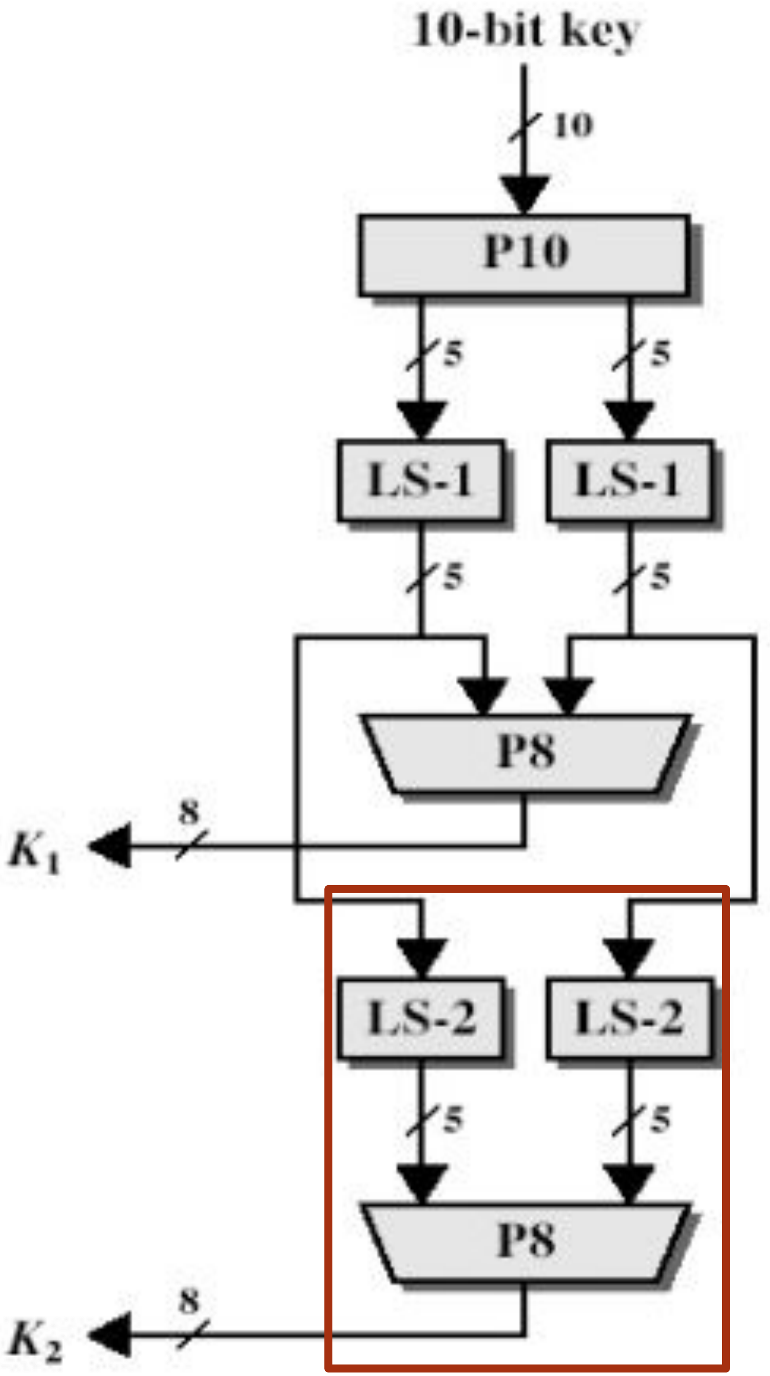
P8							
6	3	7	4	8	5	10	9

- The result is **subkey 1 (K1).**
- **SO Key 1=** **(10100100)**



For Key-2 :

- The pair of 5-bit strings produced by the two LS-1 functions in Step 2 **(00001 11000)**
- Perform a circular left shift of 2 bit positions on each string.
- So the value **(00001 11000) becomes (00100 00011).**
- Finally, P8 is applied again to produce K2.
- The **K2 is (01000011).**



Key1 and Key2

- Key= (1010000010)
- Key1= (10100100)
- Key2= (01000011)

Key Generation

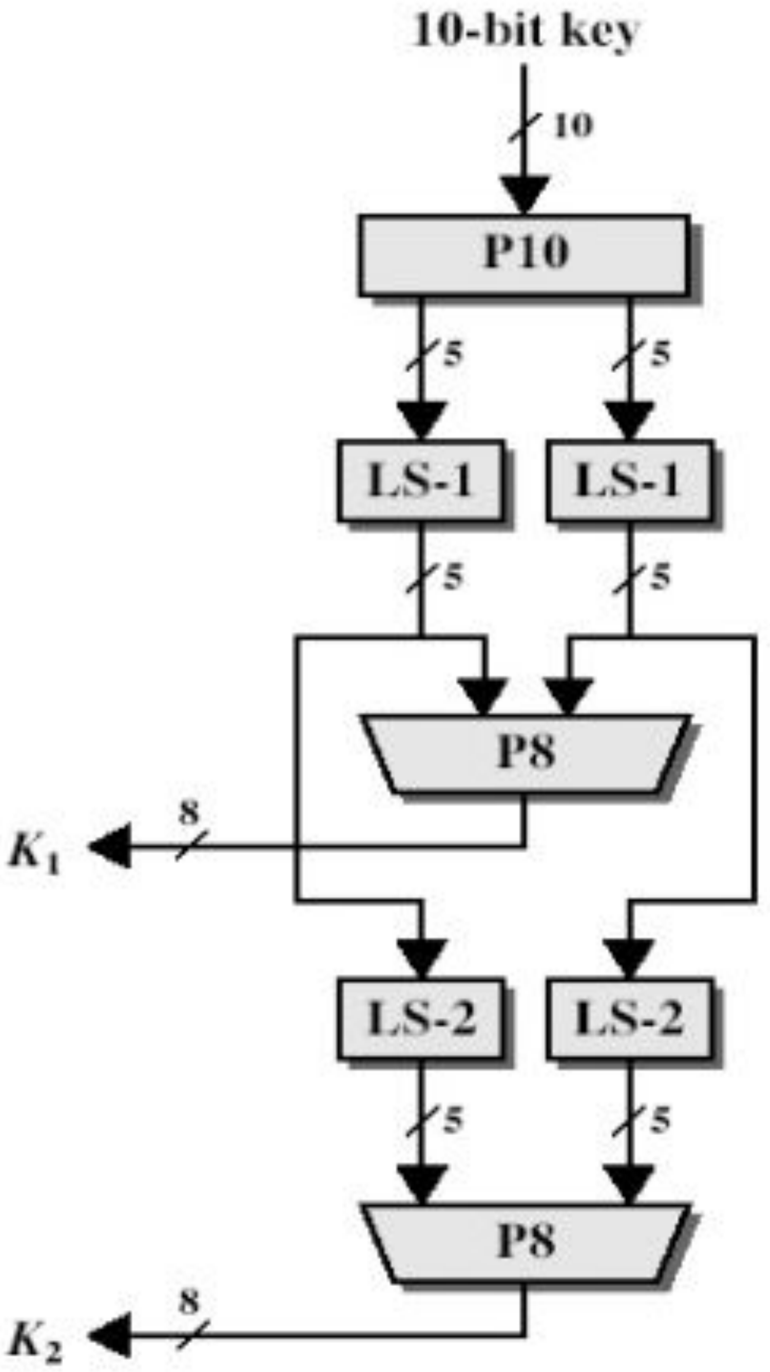
P10									
3	5	2	7	4	10	1	9	8	6

Left Shift by 1 bit

P8							
6	3	7	4	8	5	10	9

Left Shift by 2 bit

P8							
6	3	7	4	8	5	10	9



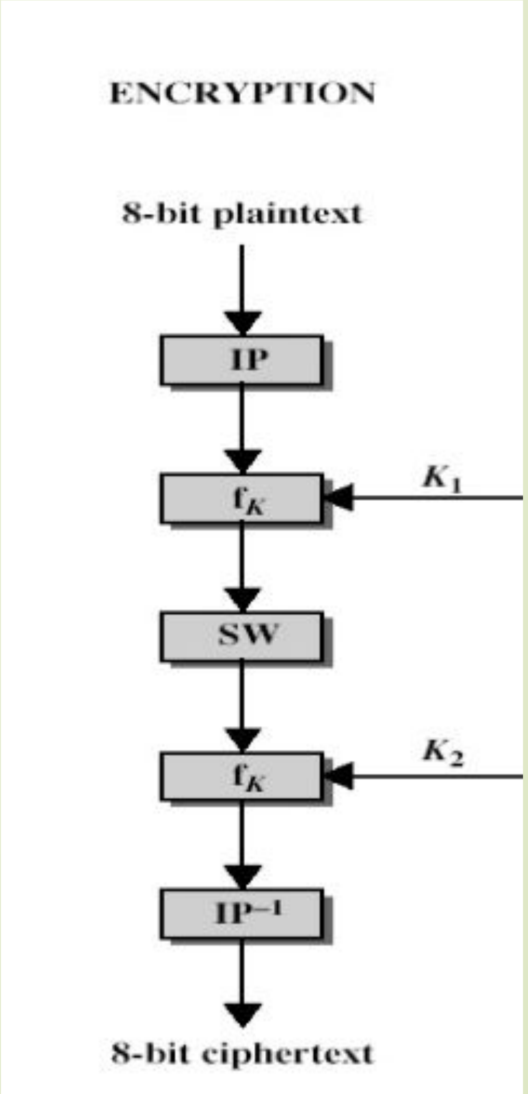
S-DES Encryption Algorithm

- **Step 1: Initial Permutation**

IP							
2	6	3	1	4	8	5	7

- **Step 5: Final Permutation**

IP –1							
4	1	3	5	7	2	8	6



The Function f_k

- The function f_k consists of a combination of permutation and substitution functions.

$$\mathbf{f_k(L, R) = (L \oplus F(R, SK), R)}$$

- L and R be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to $\mathbf{f_k}$.
- **SK** is a **subkey**.

F(R,SK)

- The first operation is an expansion/permutation operation:

E/P							
4	1	2	3	2	3	4	1

$$
\begin{array}{c|cc|c}
n_4 & n_1 & n_2 & n_3 \\
n_2 & n_3 & n_4 & n_1
\end{array}
$$

Continue...

- The 8-bit subkey K1 = (k11, k12, k13, k14, k15, k16, k17, k18) is added to this value using exclusiveOR:

$$\left[\begin{array}{c|cc|c} n_4 \oplus k_{11} & n_1 \oplus k_{12} & n_2 \oplus k_{13} & n_3 \oplus k_{14} \\ n_2 \oplus k_{15} & n_3 \oplus k_{16} & n_4 \oplus k_{17} & n_1 \oplus k_{18} \end{array}\right]$$

$$\left[\begin{array}{c|cc|c} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} \\ p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} \end{array}\right]$$

Continue...

- The first 4 bits (first row of the preceding matrix) are fed into the S-box S0 to produce a 2- bit output.
- The remaining 4 bits (second row) are fed into S1 to produce another 2-bit output.

Continue...

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Continue...

- The first and fourth input bits are treated as a 2-bit number that specify a row of the S-box, and the second and third input bits specify a column of the Sbox.
- The entry in that row and column, in base 2, is the 2-bit output. For example, if (p0,0p0,3) = (00) and (p0,1p0,2) = (10),
- then the output is from row 0, column 2 of S0, which is 3, or (11) in binary.

Continue...

- Similarly, (p1,0 p1,3) and (p1,1 p1,2) are used to index into a row and column of S1 to produce an additional 2 bits.
- Next, the 4 bits produced by S0 and S1 undergo a further permutation as follows:

P4			
2	4	3	1

Continue…

- The output of P4 is the output of the function F.

The Switch Function

- The function fK only alters the leftmost 4 bits of the input. The switch function (SW) interchanges the left and right 4 bits so that the second instance of fK operates on a different 4 bits.

IP							
2	6	3	1	4	8	5	7

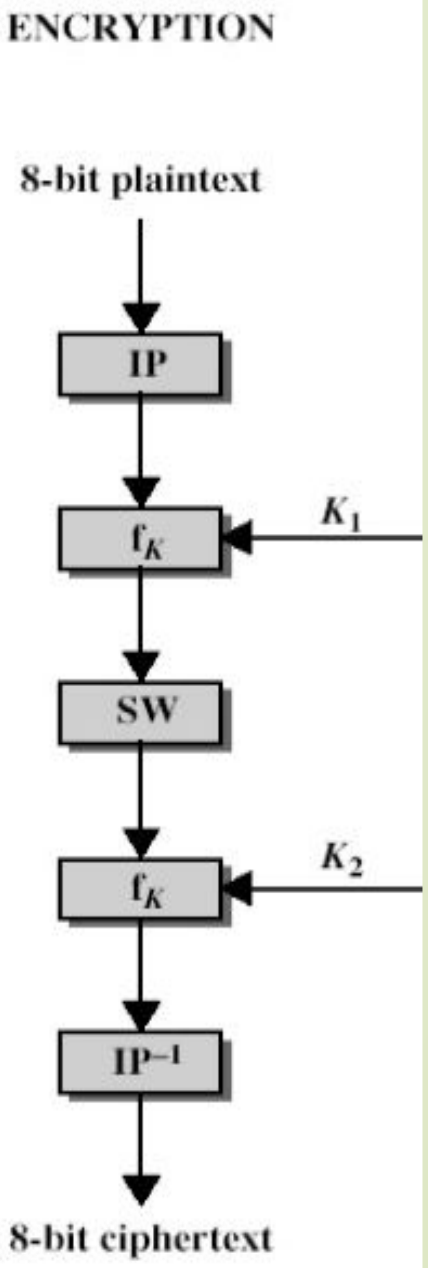
$f_k(L, R) = (L \oplus F(R, SK), R)$

F(R,SK)

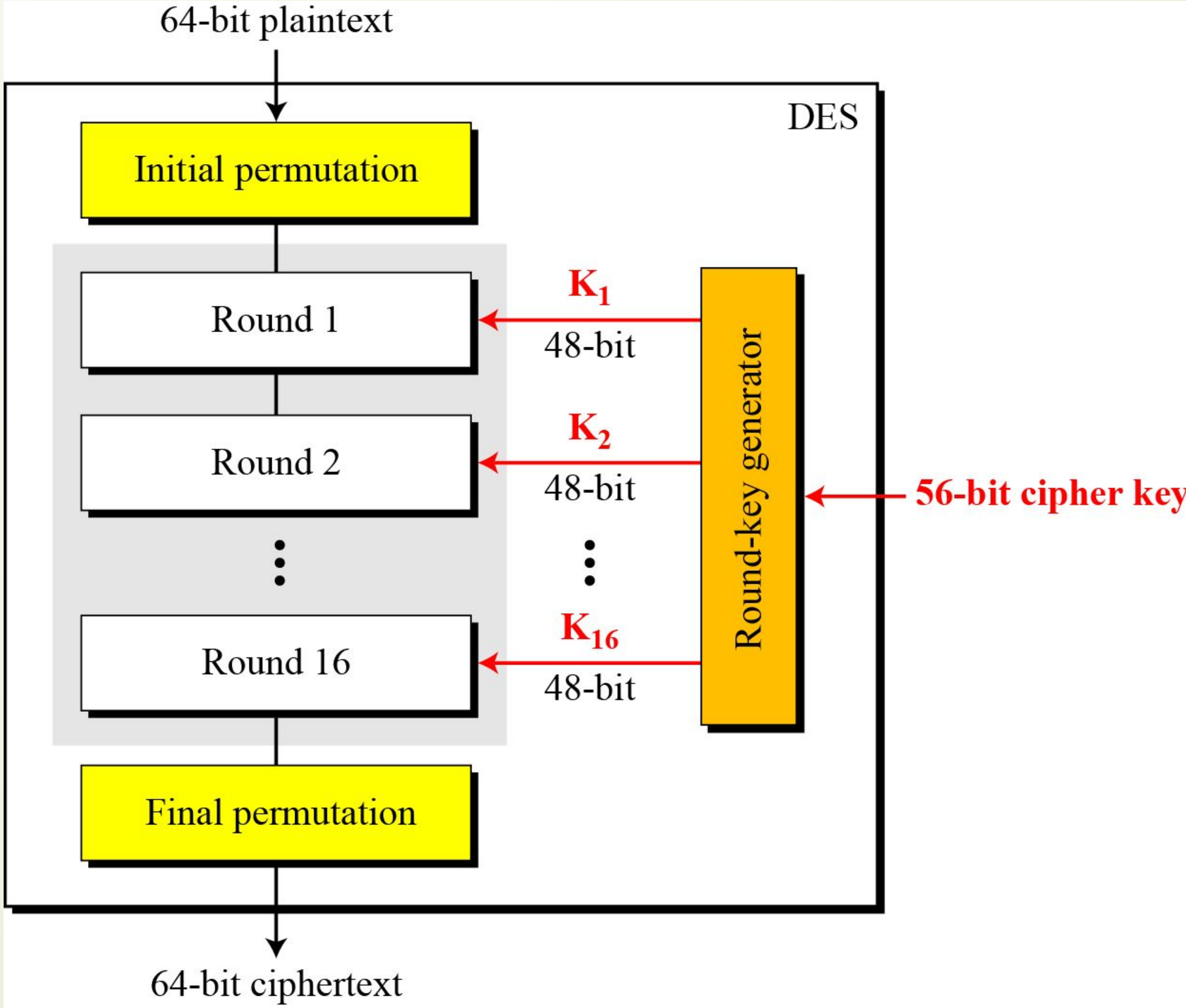
E/P							
4	1	2	3	2	3	4	1

$n_4 \oplus k_{11}$	$n_1 \oplus k_{12}$	$n_2 \oplus k_{13}$	$n_3 \oplus k_{14}$
$n_2 \oplus k_{15}$	$n_3 \oplus k_{16}$	$n_4 \oplus k_{17}$	$n_1 \oplus k_{18}$

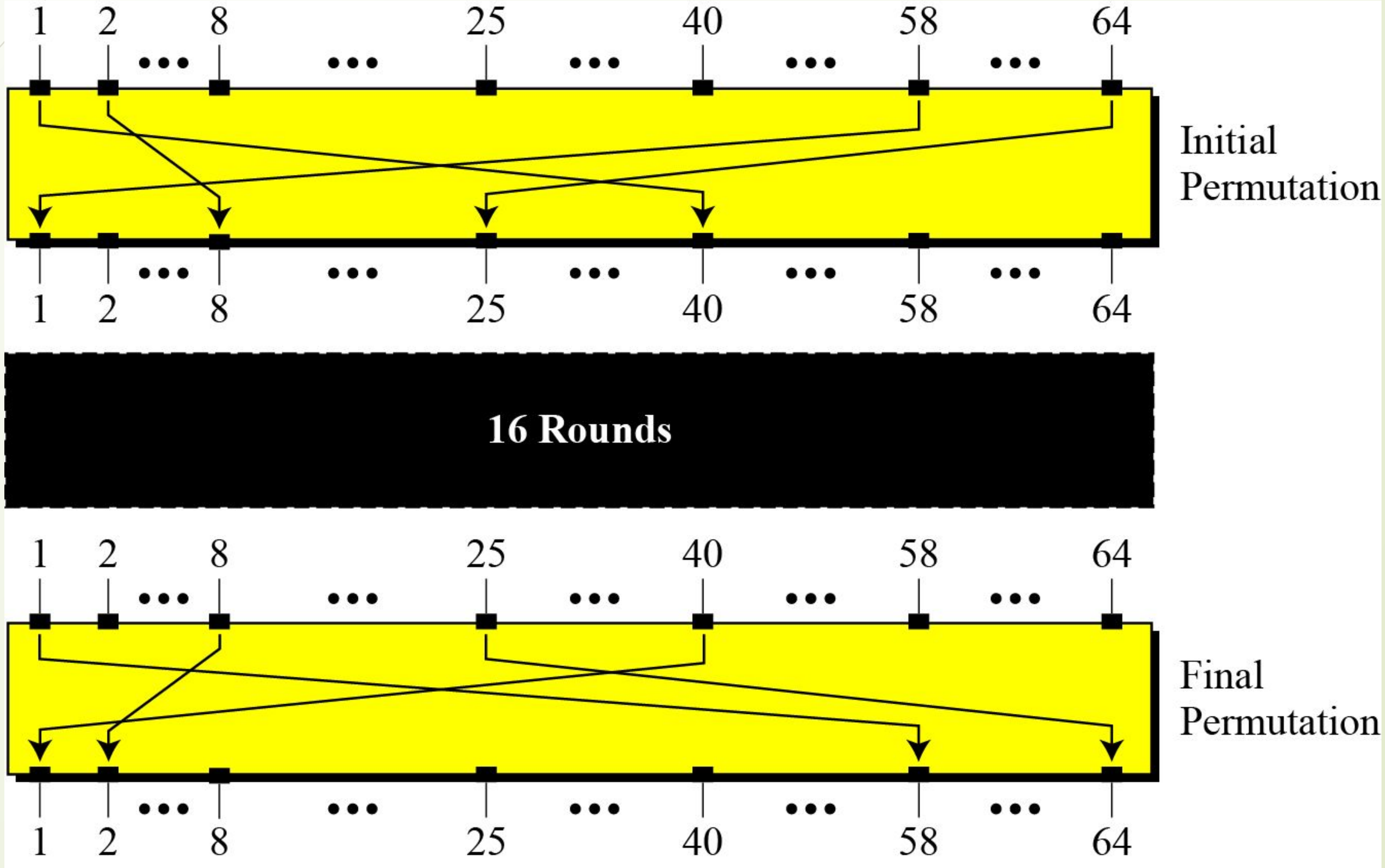
$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$



Data Encryption Standard (DES)



Initial and final permutation steps in DES



Permutation Table

Initial Permutation							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Final Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

Permutation Table

Initial Permutation								*Final Permutation*							
58	50	42	34	26	18	10	02	40	08	48	16	56	24	64	32
60	52	44	36	28	20	12	04	39	07	47	15	55	23	63	31
62	54	46	38	30	22	14	06	38	06	46	14	54	22	62	30
64	56	48	40	32	24	16	08	37	05	45	13	53	21	61	29
57	49	41	33	25	17	09	01	36	04	44	12	52	20	60	28
59	51	43	35	27	19	11	03	35	03	43	11	51	19	59	27
61	53	45	37	29	21	13	05	34	02	42	10	50	18	58	26
63	55	47	39	31	23	15	07	33	01	41	09	49	17	57	25

Find the output of the initial permutation box when the input is given in hexadecimal

0002 0000 0000 0001

0000 0080 0000 0002

Find the output of the Final permutation box when the input is given in hexadecimal

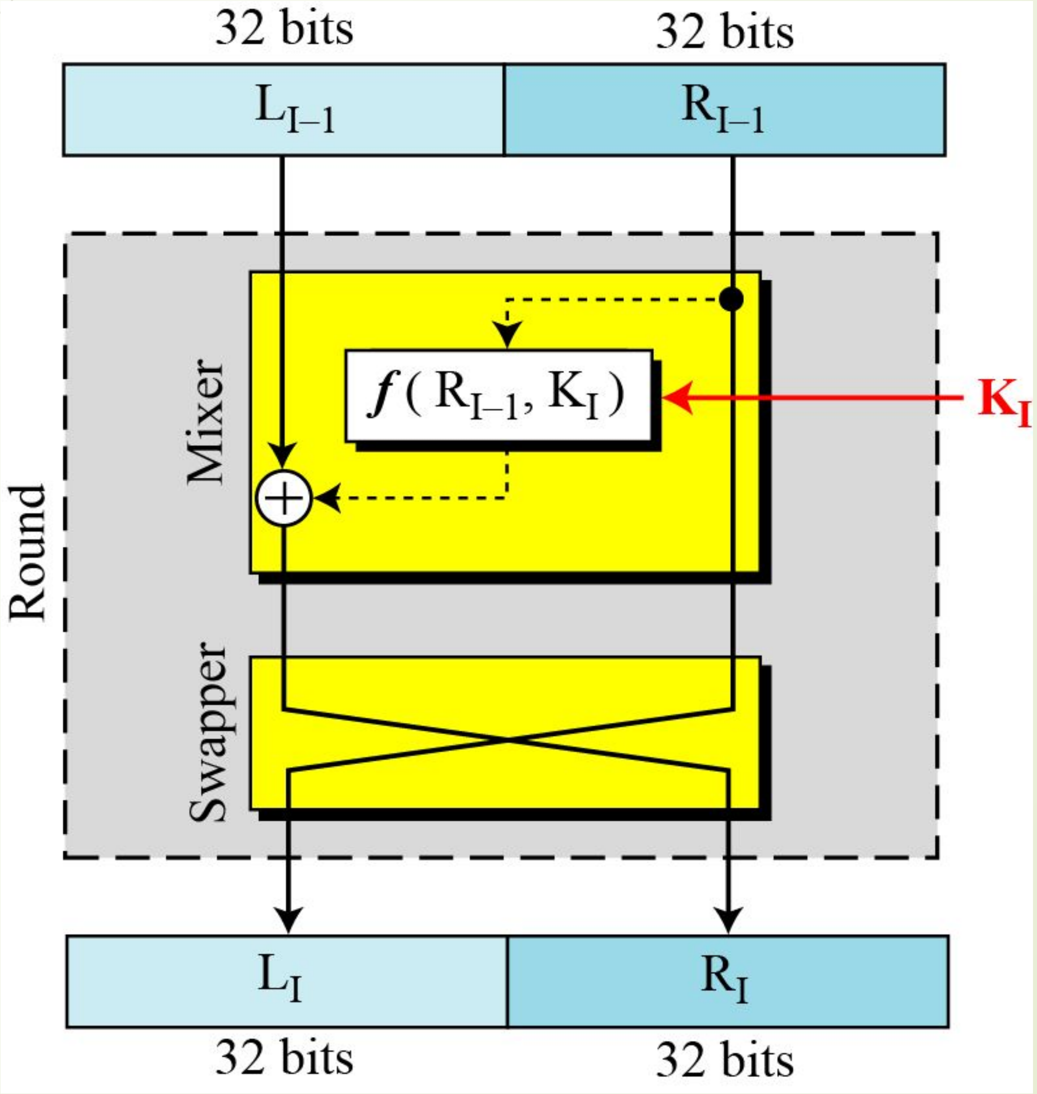
0000 0080 0000 0002

0002 0000 0000 0001

The initial and final permutations are straight P-boxes that are inverses of each other.

They have no cryptography significance in DES.

Rounds of DES

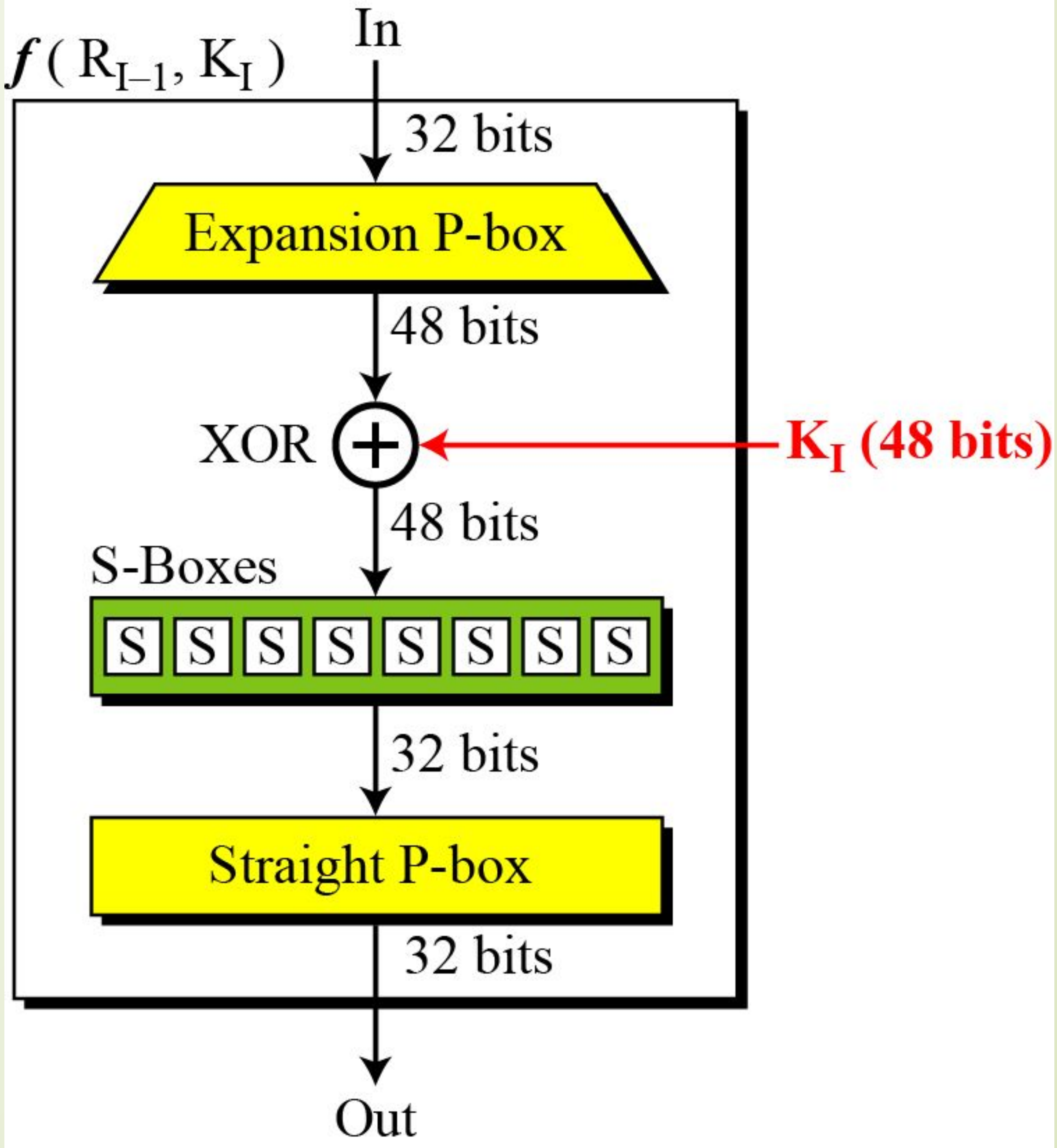


DES ***uses*** ***16 rounds.***

Each round of DES is a Feistel cipher.

DES Function

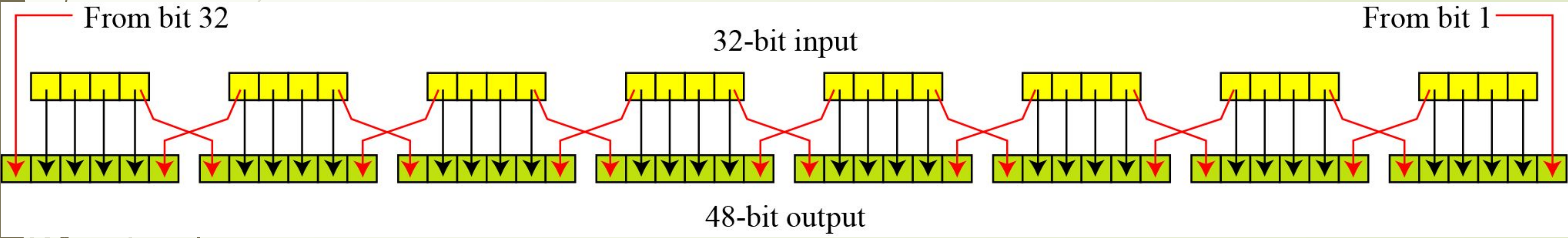
- The **heart of DES** is the **DES function.**
- The DES function applies a **48-bit key** to the rightmost 32 bits to produce a 32-bit output.



Expansion P-box

- Since **RI−1 is a 32-bit input** and **KI is a 48-bit key**, we first need to **expand RI−1 to 48 bits.**

Expansion P- Box



Expansion P Box

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

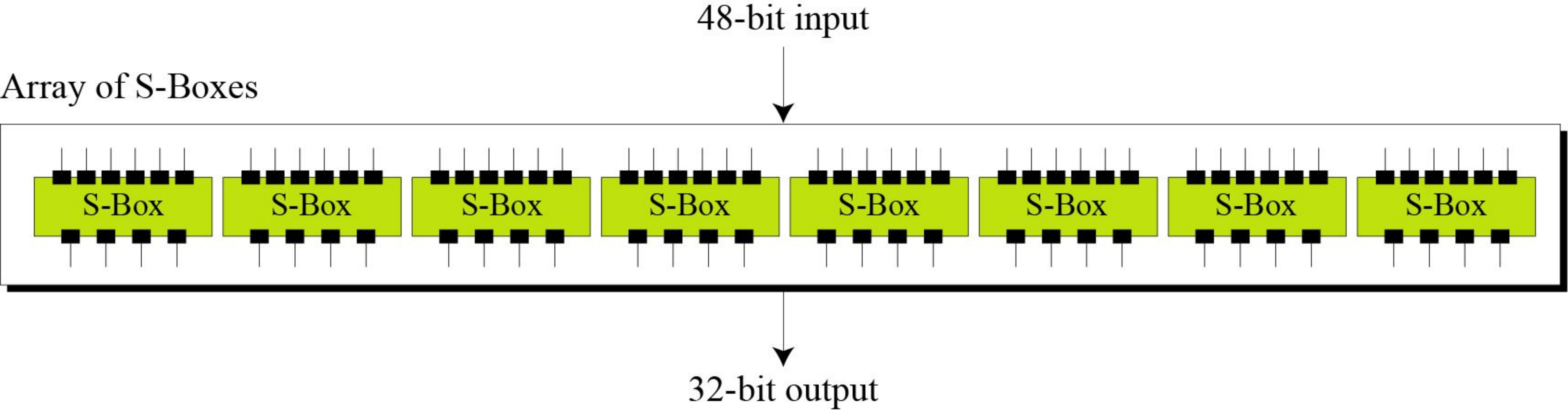
After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.

Note: Both the right section and the key are 48-bits in length.

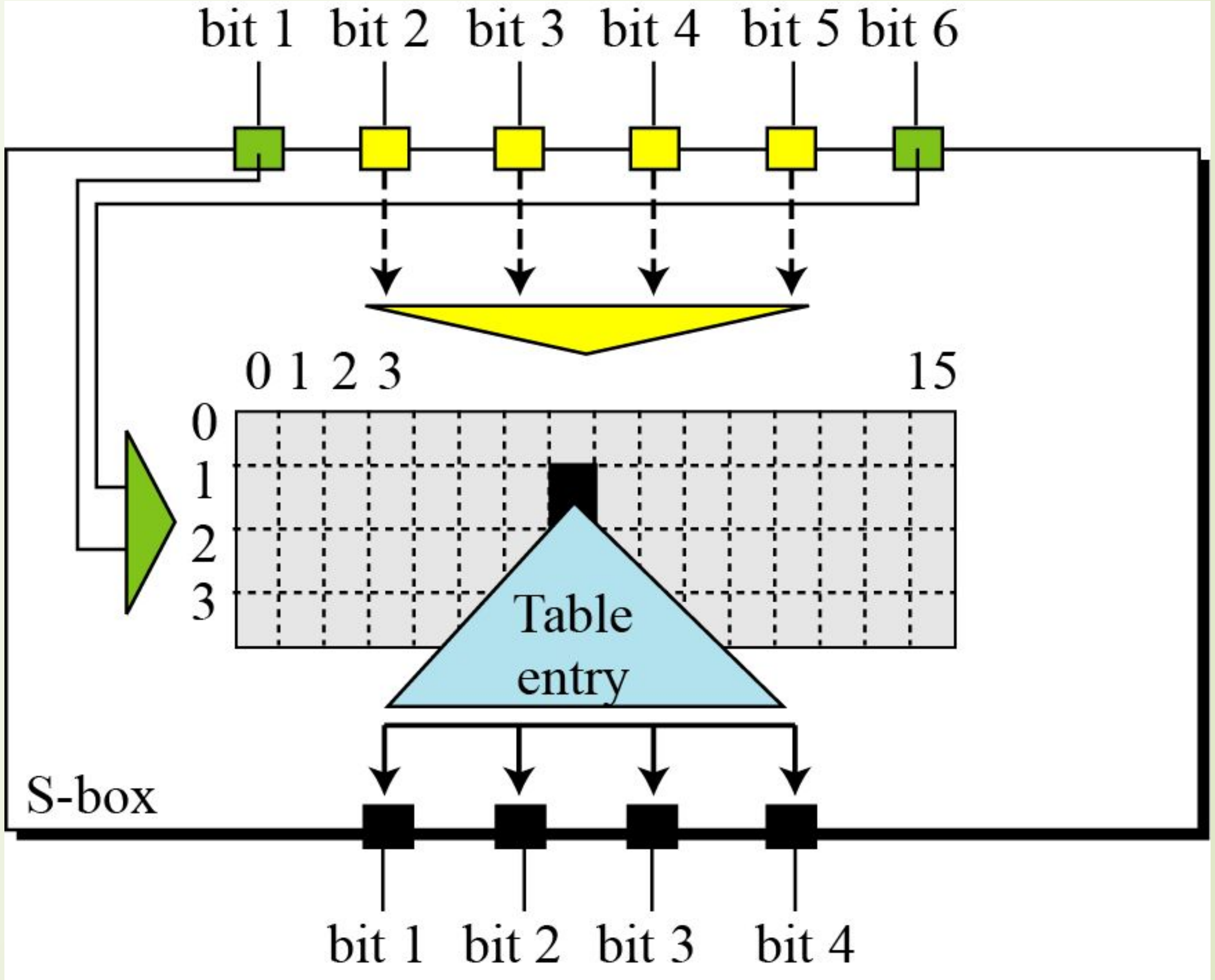
The round key is used only in this operation.

S-Box

- The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



S-Box


bit 1 bit 2 bit 3 bit 4 bit 5 bit 6
0 1 2 3
15
0
1
2
3
Table
entry
S-box
bit 1 bit 2 bit 3 bit 4

The input to given S-box 1 is 100011. What is the output?

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

The input 100011 yields the output **1100.**

Straight Permutation Table

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

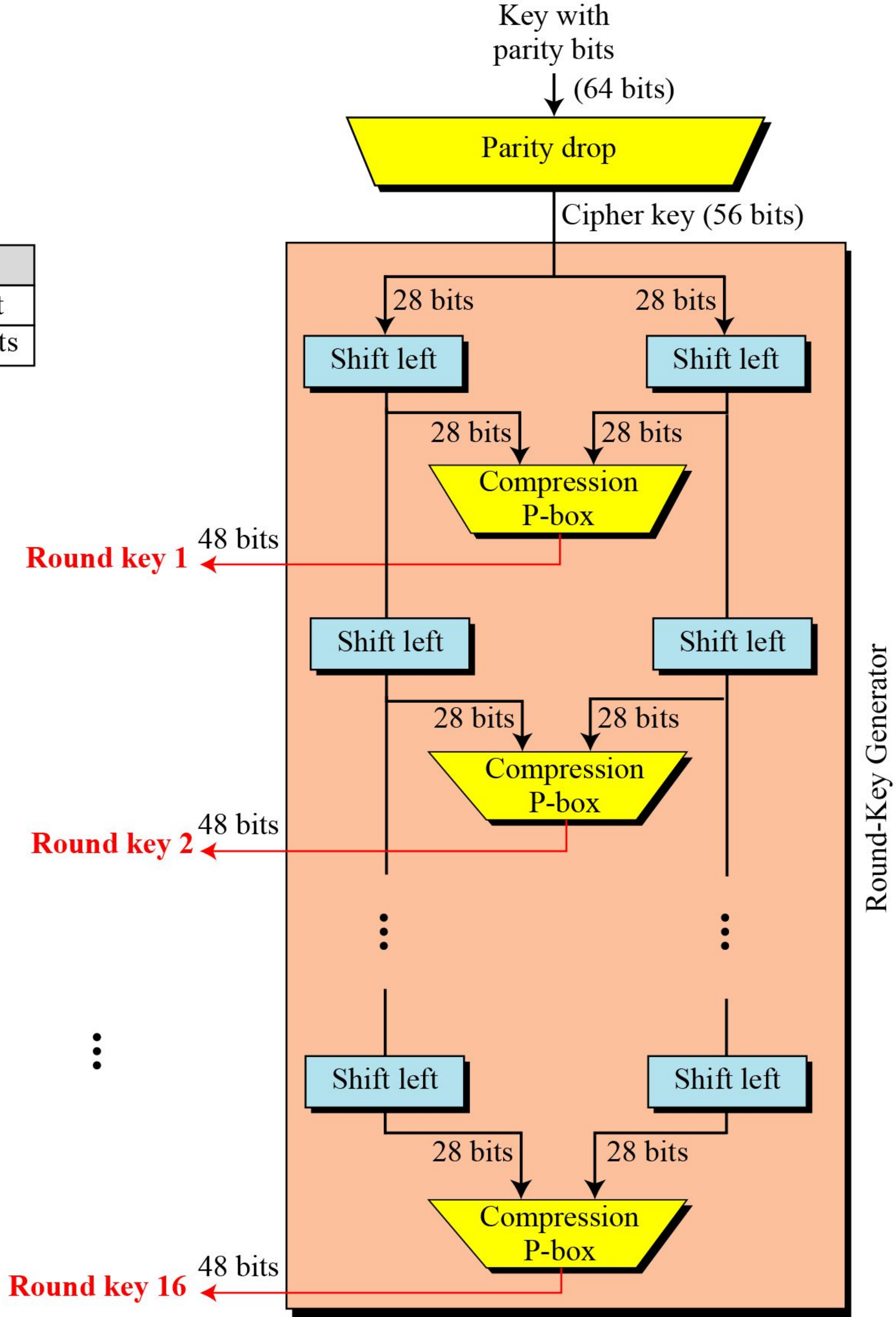
Using mixers and swappers, we can create the cipher and reverse cipher, each having 16 rounds.

- *First Approach*
- To achieve this goal, one approach is to make the last round (round 16) different from the others; it has only a mixer and no swapper.
- In the first approach, there is no swapper in the last round.
- *Alternative Approach*
- We can make all 16 rounds the same by including one swapper to the 16th round and add an extra swapper after that (two swappers cancel the effect of each other).

Key Generation

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Parity Drop

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	$\boxed{28}$	$\boxed{29}$	$\boxed{30}$	$\boxed{31}$	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
$\boxed{57}$	$\boxed{58}$	$\boxed{59}$	$\boxed{60}$	$\boxed{61}$	$\boxed{62}$	$\boxed{63}$	64

$\boxed{57}$	49	41	33	25	17	9	1
$\boxed{58}$	50	42	34	26	18	10	2
$\boxed{59}$	51	43	35	27	19	11	3
$\boxed{60}$	52	44	36	$\boxed{63}$	55	47	39
$\boxed{31}$	23	15	7	$\boxed{62}$	54	46	38
$\boxed{30}$	22	14	6	$\boxed{61}$	53	45	37
$\boxed{29}$	21	13	5	$\boxed{28}$	20	12	4

Parity Drop

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Number of bits shifts

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Key-compression table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Desire Properties of Block Cipher

- **Avalanche Effect :** a small change in the plaintext should create a significant change in ciphertext.
- **Completeness Effect :** each bit of the ciphertext needs to depend on many bits on the plaintext.

DES Analysis- Avalanche Effect and Completeness

DES performs strong with regards to Avalanche effect.

Diffusion and confusion produced by D-box and S-Boxes in DES, show a VERY STRONG Completeness Effect.

Design Criteria for DES

Design Criteria for DES

- **S-Box**
  - *The entries of each row are permutations of values between 0 to 15.*
  - *If we change a single bit in the input, two or more bits will be changed in the output.*
  - *If two inputs to an s-box differ only in middle two bits(bit 3 and 4), the output must differ in at least two bits.*
  - *If the inputs to an s-box differ in the first two bits and the same in last two bits, the output must be different.*
  - *In any S-box, if a single bit is held constant and the other bits are changed randomly, the differences between the number of 0s and 1s are minimized.*

Continue…

- **D-Boxes**
  - *There are two types D-Boxes between S-boxes of two subsequent rounds.*
    - *Straight D-Box*
    - *Expansion D-Box*

Continue…

- **Number of Rounds**
  - *16 Rounds*
  - *DES versions less than 16 rounds are venerable to known plain text attack, that's why sixteen rounds are recommended to use in DES.*

DES Weakness

- S-Box
  - In S-box 4, the last three output bits can be derived in the same way as the first output bit by complementing some of the input bits.
  - Two specifically chosen inputs to an S-box array can create the same output.
  - It is possible to obtain the same output in a single round by changing bits in only three neighboring S-boxes.
- D-boxes
  - The initial and final permutations; these have no security benefits.
  - In the expansion permutation (inside the function), the first and fourth bits of every 4-bit series are repeated.

Weakness in Cipher Key

- The most serious weakness of DES is in its key size (56 bits). To perform a brute force attack on a given ciphertext block, the adversary needs to check **2^{56} keys**.

Weak Key

- 4 keys out of 256 keys are weak keys.
- A weak is the one that, after parity drop operation consists either of all 0sm all 1s or half 0s and half 1s.
- The round keys created from any of these weak keys are the same and have the same pattern as the cipher key.
- If we encrypt a block with a weak key and subsequently encrypt the result with same weak key, we get the original block.

Keys before parities drop (64 bits)	*Actual key (56 bits)*
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF

Semi weak Keys

- There are six key pairs that are called semi-weak keys.

First key in the pair	*Second key in the pair*
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E1 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

Continue…

A semi-weak key creates only two different round keys and each of them is repeated eight times. In addition, the round keys created from each pair are the same with different orders.

Round key 1	9153E54319BD	6EAC1ABCE642
Round key 2	6EAC1ABCE642	9153E54319BD
Round key 3	6EAC1ABCE642	9153E54319BD
Round key 4	6EAC1ABCE642	9153E54319BD
Round key 5	6EAC1ABCE642	9153E54319BD
Round key 6	6EAC1ABCE642	9153E54319BD
Round key 7	6EAC1ABCE642	9153E54319BD
Round key 8	6EAC1ABCE642	9153E54319BD
Round key 9	9153E54319BD	6EAC1ABCE642
Round key 10	9153E54319BD	6EAC1ABCE642
Round key 11	9153E54319BD	6EAC1ABCE642
Round key 12	9153E54319BD	6EAC1ABCE642
Round key 13	9153E54319BD	6EAC1ABCE642
Round key 14	9153E54319BD	6EAC1ABCE642
Round key 15	9153E54319BD	6EAC1ABCE642
Round key 16	6EAC1ABCE642	9153E54319BD

Possible Weak keys

- There are also 48 keys that are called possible weak keys.
- A possible weak key is a key that creates only four distinct round keys; in other words, the sixteen round keys are divided into four groups and each group is made of four equal round key.

What is the probability of randomly selecting a weak, a semi-weak, or a possible weak key?

- (4 + 12 + 48) =64 keys which falls under the categories of Weak, semi-weak and possible weak keys.
- Total keys are 2^{56}

Security of DES

- Differential Cryptanalysis – Chosen Plain text attack
- Linear Cryptanalysis- Known Plain text attack

References

- Cryptography and network security – Behrouz a forouzan, debdeep mukhopadhyay

Any Questions??

Thank You